ИНФОРМАТИКА

2008 **январь-март** **№ 1**

УДК 004.93'1

М.Н. Бобов, П.М. Буй

ОЦЕНКА УРОВНЯ ЗАЩИЩЕННОСТИ ГОЛОСОВОГО СРЕДСТВА АУТЕНТИФИКАЦИИ

Рассматривается задача оценки уровня защищенности средств аутентификации различных классов. Производится вывод аналитической формулы для оценки уровня защищенности средства аутентификации по образцу голоса и дается пример расчета уровня защищенности конкретного средства аутентификации.

Введение

Средство аутентификации – это программный модуль или аппаратно-программное устройство, которое обеспечивает проверку подлинности субъекта, т. е. устанавливает, является ли он тем, за кого себя выдает.

Процесс проверки подлинности субъекта зависит от метода, который используется в средстве аутентификации. Известные методы опознания объединены в три класса, которые базируются:

– на условных, заранее присваиваемых признаках (сведениях), известных субъекту (что знает субъект);

– физических средствах, действующих аналогично физическому ключу (что имеет субъект);

– индивидуальных характеристиках субъекта, его физических данных, позволяющих выделить его среди других лиц (что присуще субъекту) [1].

В средствах аутентификации, относящихся к первым двум классам, проверка подлинности субъекта осуществляется на основании предоставляемого им пароля или ключа. В средствах аутентификации третьего класса проверка подлинности субъекта осуществляется на основании предоставляемого им биометрического признака. В качестве биометрического признака используются:

– отпечаток пальца;
– форма ладони;
– сетчатка глаза;
– радужная оболочка глаза;
– форма лица;
– термограмма лица;
– почерк;
– голос;
– подпись.

В процессе проверки субъекта выясняется, что предоставляемый им пароль или ключ либо идентичен эталонному, хранящемуся в базе данных средства аутентификации (в этом случае субъект считается подлинным), либо не идентичен (субъект считается ложным).

Биометрические средства аутентификации отличаются тем, что предоставляемый субъектом биометрический признак никогда не будет полностью идентичен эталонному. Для данного класса средств аутентификации вводится понятие меры близости предоставляемого признака с эталонным [2]. Для принятия решения об аутентичности субъекта используется понятие порога меры близости. Порог меры близости – это такое значение меры близости предоставляемого субъектом признака с эталонным, при непревышении которого субъект считается «своим», а при превышении – «чужим».

1. Оценка уровня защищенности средств аутентификации

Для оценки уровня защищенности средств аутентификации используется вероятность пропуска «чужого» субъекта, которая для небиометрических методов определяется как вероятность подбора с первой попытки пароля или ключа [1]:

$$P_{\text{ïï}} = \frac{1}{A^c}; \tag{1}$$

$$P_{\text{ïê}} = \frac{1}{2^k}, \tag{2}$$

где $P_{\text{ПП}}$ – вероятность подбора пароля;
$P_{\text{ПК}}$ – вероятность подбора ключа;
A – алфавит, используемый в пароле;
c – количество символов пароля;
k – длина ключа в битах.

Для биометрических средств аутентификации аналитические выражения для определения вероятности пропуска «чужого» субъекта могут быть получены только индивидуально для каждого из набора признаков с использованием ряда приближений и допущений.

В последнее время можно отметить возросший интерес к проблеме аутентификации по голосу. На сегодняшний день созданы десятки различных систем идентификации по голосу, имеющих различные параметры и требования к процессу аутентификации в зависимости от конкретных задач.

Рассмотрим одно из биометрических средств аутентификации на основе распознавания голоса [3]. В данном средстве аутентификации каждый субъект при обучении трижды производит запись образца своей речи. По каждому из трех образцов отдельно определяются векторы речевых признаков, представляющие характерные параметры входного речевого сигнала. В данном средстве аутентификации в качестве векторов речевых признаков используются наборы кепстральных коэффициентов линейного предсказания, определяемых с помощью метода линейного предсказания. Методом векторного квантования векторы речевых признаков формируются в три матрицы эталонных признаков, каждая из которых соответствует определенному образцу речи субъекта. Эталонные матрицы хранятся в базе данных средства аутентификации. В процессе опознания парольная фраза субъекта проходит описанную выше обработку, в результате чего формируется текущая матрица речевых признаков, которая сравнивается с эталонными. Субъект признается аутентичным в том случае, если меры близости между сформированной матрицей и хотя бы двумя эталонными матрицами из трех не превышают заданный порог.

Определим аналитическое выражение для расчета вероятности пропуска «чужого» субъекта для указанного средства аутентификации.

Выходной сигнал речевого тракта представляет собой свертку сигнала возбуждения и импульсного отклика голосового тракта:

$$x(t) = e(t) * h(t), \tag{3}$$

где $x(t)$ – входной речевой сигнал;
$e(t)$ – сигнал возбуждения;
$h(t)$ – импульсный отклик голосового тракта;
t – время;
$*$ – знак свертки.

Эту систему можно рассмотреть в частотной области, тогда преобразование Фурье речевого сигнала равно произведению преобразований Фурье функции возбуждения и импульсного отклика голосового тракта:

$$X(\omega) = E(\omega) \cdot H(\omega), \tag{4}$$

где ω – частота.

Спектр периодической возбуждающей последовательности $E(\omega)$ линейчатый, его гармоники отстоят друг от друга на $2\pi/T_в$, где $T_в$ – период сигнала возбуждения. Частотная характеристика голосового тракта $H(\omega)$ является сравнительно гладкой функцией частоты. При создании различных звуков форма речевого тракта изменяется, при этом изменяется и форма огибающей спектра речевого сигнала во времени. Следовательно, чтобы проводить корректный спектральный анализ речи, следует иметь в виду кратковременный спектральный анализ на интервале времени 10–30 мс, допуская, что за этот временной интервал речевой тракт не успевает существенно изменить свою геометрию за счет перестройки артикуляторов [3].

Таким образом, речевой сигнал удобнее представлять не в виде непрерывной функции времени t, а одномерным оцифрованным сигналом $x(n)$, где n – порядковый номер интервала времени [4]. В данном средстве аутентификации субъект, создавая эталонные матрицы, трижды записывает свой звуковой пароль, формируя тем самым три матрицы S_1, S_2 и S_3 размерности $T\times L$, где L – количество кепстральных коэффициентов, которые используются в процессе создания матриц; T – количество интервалов времени в эталонных записях, которые формируются методом векторного квантования «k-средних». Эталонные матрицы имеют вид

$$S_j = \begin{bmatrix} c_1(1)_j & c_2(1)_j & \cdots c_T(1)_j \\ c_1(2)_j & c_2(2)_j & \cdots c_T(2)_j \\ \cdots & & \\ c_1(L)_j & c_2(L)_j & \cdots c_T(L)_j \end{bmatrix}, \tag{5}$$

где S_j – эталонная матрица, j=1, 2, 3;

$c_n(m)_j$ – m-й кепстральный коэффициент n-го интервала времени j-й эталонной матрицы, определяемый по формуле [5]

$$c_n(m)_j = \frac{1}{L}\sum_{k=1}^{L} \lg\left|X_n(k)_j\right| e^{j\frac{2\pi}{L}km};\ n=1,2,...,T;\ m=1,2,...,L. \tag{6}$$

Здесь $X_n(k)_j$ – преобразование Хартли для j-й эталонной речевой последовательности;

k – частотный индекс Хартли.

Аналогичным образом входная речевая последовательность методом векторного квантования преобразуется в матрицу S размерности $T\times L$.

В связи с этим текущая матрица признаков субъекта имеет вид

$$S = \begin{bmatrix} c_1(1) & c_2(1) & \cdots c_T(1) \\ c_1(2) & c_2(2) & \cdots c_T(2) \\ \cdots & & \\ c_1(L) & c_2(L) & \cdots c_T(L) \end{bmatrix}, \tag{7}$$

где $c_z(m)$ – m-й кепстральный коэффициент z-го интервала времени текущей матрицы признаков субъекта, определяемый по формуле

$$c_z(m) = \frac{1}{L}\sum_{k=1}^{L} \lg\left|X_z(k)\right| e^{j\frac{2p}{L}km},\ z=1,2,...,\mathrm{T},\ m=1,2,...,L. \tag{8}$$

Для сравнения сформированной по голосу субъекта матрицы с эталонными формируются три матрицы мер близости D_1, D_2, D_3 с размерностями $T\times T$, такие, что

$$d_j(n,z) = \sum_{m=1}^{L} w_m (S_{jn,m} - S_{z,m})^2,\ n,z=1,2,...,T,\ m=1,2,...,L, \tag{9}$$

где w_m – обратное значение дисперсии m-го кепстрального коэффициента входной речевой последовательности.

Затем из каждой матрицы выбираются T значений, которые соответствуют минимальным мерам близости так, что каждому столбцу и каждой строке матрицы может принадлежать только одно из выбранных значений. Окончательно мера близости d между предоставляемой матрицей и эталонной определяется как среднее арифметическое из T выбранных значений.

Если окончательная мера близости меньше заданного порога g, то по данной эталонной матрице субъект признается «своим». Если тестируемую парольную фразу предоставил «чужой» субъект и по двум из трех матриц мер близости он будет признан «своим», то произойдет пропуск данного «чужого» субъекта.

Значения матриц мер близости зависят от значений матриц кепстральных коэффициентов. В работе [3] приведены гистограммы распределений кепстральных коэффициентов на множестве субъектов. Кепстральные коэффициенты имеют нормальный закон распределения с разными математическими ожиданиями. Математические ожидания большинства нормальных распределений кепстральных коэффициентов на множестве субъектов, согласно представленным в [3] гистограммам, близки к нулю. Математические ожидания нормальных распределений первого и второго кепстральных коэффициентов на множестве субъектов смещены относительно нуля.

Таким образом, законы распределения случайных величин значений матриц D_1, D_2, D_3 не определены и неизвестны в литературе, поэтому для определения этих значений требуется произвести длительные эксперименты и сложные аналитические расчеты. Естественно, в таком случае формулы для расчета вероятности пропуска «чужого» субъекта должны полностью включать значения матриц мер близости, что делает их достаточно громоздкими.

Поэтому для упрощения данных формул произведем нормирование матриц мер близости, в результате чего случайная величина значений этих матриц из непрерывной неограниченной реализации преобразуется в непрерывную реализацию на отрезке [0, 1]. Для построения нормированных матриц мер близости Dn_1, Dn_2, Dn_3 воспользуемся следующей тригонометрической функцией:

$$f(x) = \frac{2}{\pi}\left|\operatorname{arctg}(x)\right|. \tag{10}$$

Нормирование с использованием данной тригонометрической функции в силу ее свойств позволяет выделить значения матриц мер близости, которые близки к нулю и влияют на определение субъекта «своим». Тогда значения нормированных матриц мер близости будут вычисляться следующим образом:

$$dn_j(n,z) = \frac{2}{\pi}\left|\operatorname{arctg}(d_j(n,z))\right|. \tag{11}$$

Аналогичное нормирование необходимо произвести с порогом g. Нормированное значение порога меры близости Δ вычисляется по формуле

$$\Delta = \frac{2}{\pi}\left|\operatorname{arctg}(g)\right|. \tag{12}$$

Непрерывность реализации случайной величины значений нормированных матриц мер близости на отрезке [0, 1] предполагает бесконечное количество значений этой случайной величины. В связи с этим проведем дискретизацию нормированных значений матриц мер близости с шагом Δ. В результате дискретизации все значения нормированных матриц мер близости, которые были меньше Δ, становятся равными нормированному порогу меры близости.

Наличие в дискретной нормированной матрице мер близости значения, равного нормированному порогу меры близости, означает, что кепстральные коэффициенты временного интервала, номер которого равен номеру строки, эталонной речевой последовательности соответствуют кепстральным коэффициентам временного интервала, номер которого равен номеру столбца, входной речевой последовательности. Если в дискретной нормированной матрице мер близости найдутся T таких значений, каждое из которых принадлежит своей строке и своему столбцу, то кепстральные коэффициенты всех временных интервалов эталонной речевой последовательности попарно будут соответствовать кепстральным коэффициентам временных интервалов входной речевой последовательности.

Следовательно, субъект будет признан «своим» по дискретной нормированной матрице мер близости, если в ней найдутся T значений, равных нормированному порогу меры близости, таких, что каждому столбцу и каждой строке матрицы будет принадлежать только одно из выбранных значений.

После нахождения каждый раз одного из значений, равного Δ, из области поиска в нормированной дискретной матрице мер близости убираются одна строка и один столбец, которым принадлежит ячейка с найденным значением.

Вероятность того, что любой субъект будет признан «своим» по дискретной нормированной матрице мер близости, будет равна

$$P_{\Delta} = \prod_{i=T}^{1} P_{\Delta i}, \tag{13}$$

где i – переменная, значение которой равно количеству строк или столбцов квадратной матрицы; $i=T, T-1, \ldots, 1$;

$P_{\Delta i}$ – вероятность того, что найдется хотя бы одно значение дискретной нормированной матрицы мер близости с размерностью $i \times i$ (с учетом использованных столбцов и строк), равное Δ. Указанная вероятность может быть определена по формуле

$$P_{\Delta i} = \sum_{h=1}^{i^2} \frac{(i^2)!}{h! \cdot (i^2 - h)!} \cdot \Delta^h \cdot (1-\Delta)^{(i^2-h)}, \tag{14}$$

где h – переменная, значение которой равно количеству ячеек в матрице размером $i \times i$; $h=1, 2, \ldots, i^2$.

Формулы вероятностей того, что субъект будет признан «своим» по первой, второй или третьей дискретным нормированным матрицам мер близости соответственно, будут иметь вид [6]

$$P_j = \prod_{i=T}^{1} \sum_{h=1}^{i^2} \frac{(i^2)!}{h! \cdot (i^2 - h)!} \cdot \Delta^h \cdot (1-\Delta)^{(i^2-h)}. \tag{15}$$

Вероятностью пропуска «чужого» субъекта для данного средства аутентификации будет являться вероятность того, что в двух из трех дискретных нормированных матрицах мер близости найдется T значений, равных нормированному порогу меры близости Δ, таких, что каждому столбцу и каждой строке данной матрицы будет принадлежать только одно из выбранных значений.

Тогда формула вероятности пропуска «чужого» субъекта имеет вид

$$P_{\text{ПГ}} = P_1 \cdot P_2 \cdot (1-P_3) + P_1 \cdot P_3 \cdot (1-P_2) + P_2 \cdot P_3 \cdot (1-P_1) + P_1 \cdot P_2 \cdot P_3. \tag{16}$$

Так как размерности всех трех дискретных нормированных матриц мер близости одинаковы, вероятности того, что любой субъект будет признан «своим» по первой, второй или третьей дискретным нормированным матрицам мер близости, будут равны

$$P_1 = P_2 = P_3 = P_{\Delta}. \tag{17}$$

Используя выражение (17), получим

$$P_{\text{і}\text{ä}} = P_1 \times P_2 \times (1 - P_3) + P_1 \times P_3 \times (1 - P_2) + P_2 \times P_3 \times (1 - P_1) + \\ + P_1 \times P_2 \times P_3 = 3 \times P_\Delta^2 \times (1 - P_\Delta) + P_\Delta^3, \quad (18)$$

где вероятности P_1, P_2 и P_3 определяются по формулам (15).

2. Пример расчета уровня защищенности средства аутентификации по образцу голоса

Примем следующие исходные данные для расчета уровня защищенности:

количество интервалов времени в тестируемой речевой последовательности и в эталонных записях (T) согласно [3] – 32;

количество кепстральных коэффициентов (L), которые используются в процессе создания матриц S, S_1, S_2, S_3, как это рекомендовано в [3], – 14;

порог меры близости (d) на основании анализа представленных в [3] гистограмм распределений кепстральных коэффициентов на множестве субъектов – 0,1.

В данном случае согласно формуле (12) нормированный порог меры близости

$$\Delta = \frac{2}{\pi}\left|\text{arctg}(0{,}1)\right| = 0{,}063.$$

Вероятность того, что любой субъект будет принят «своим» по одной из трех дискретных нормированных матриц мер близости, будет равна

$$P_\Delta = \prod_{i=32}^{1} \sum_{j=1}^{i^2} \frac{(i^2)!}{j! \cdot (i^2 - j)!} \cdot 0{,}063^j \cdot 0{,}937^{(i^2 - j)} = 2{,}9 \cdot 10^{-3},$$

тогда вероятность пропуска «чужого» субъекта

$$P_{\text{ПГ}} = 3 \cdot (2{,}9 \cdot 10^{-3})^2 \cdot (1 - 2{,}9 \cdot 10^{-3}) + (2{,}9 \cdot 10^{-3})^3 = 2{,}52 \cdot 10^{-5}.$$

Заключение

Полученная аналитическая формула для расчета уровня защищенности представленного биометрического средства аутентификации по образцу голоса позволяет произвести анализ эффективности данного средства аутентификации по сравнению с прочими биометрическими и небиометрическими средствами аутентификации.

Полученное значение вероятности пропуска «чужого» субъекта данным средством аутентификации показывает, что уровень защищенности рассмотренного средства аутентификации несколько ниже уровня защищенности небиометрического средства аутентификации, проверка подлинности субъекта в котором осуществляется на основании предоставляемого им пятизначного цифрового пароля.

Список литературы

1. Бобов, М.Н. Обеспечение безопасности информации в телекоммуникационных системах / М.Н. Бобов, В.К. Конопелько. – М.: БГУИР, 2002. – 164 с.

2. Кухарев, Г.А. Биометрические системы: методы и средства идентификации личности человека / Г.А. Кухарев. – СПб.: Политехника, 2001. – 240 с.

3. Рылов, А.С. Анализ речи в распознающих системах / А.С. Рылов. – Минск: Бестпринт, 2003. – 264 с.

4. Рабинер, Л.Р. Цифровая обработка речевых сигналов / Л.Р. Рабинер, Р.В. Шафер. – М.: Радио и связь, 1981. – 495 с.

5. Оппенгейм, А.В. Цифровая обработка сигналов / А.В. Оппенгейм, Р.В. Шафер. – М.: Связь, 1979. – 416 с.

6. Пугачев В.С. Введение в теорию вероятностей / В.С. Пугачев. – М.: Наука, 1968. – 368 с.

Поступила 06.07.07

Белорусский государственный университет
информатики и радиоэлектроники,
Минск, П. Бровки, 6
e-mail: pashabuoy@rambler.ru

M.N. Bobov, P.M. Bui

ESTIMATION OF SECURITY LEVEL OF VOICE BASED AUTHENTIFICATION

A task of security level estimation of various classes authentification tools is considered. An analytical formula is proposed for security level evaluation of voice based authentification tools. An example of security level evaluation for a concrete authentification tool is given.